AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application:

Listing of Claims:

1. (Currently Amended) A system ~~for authenticating a user's signature, the system~~ comprising:

first extraction means for extracting first angle data and first distance data relating to different parts of [[the]] a user's signature to obtain a signature trace;

normalization means for generating a normalized signature trace by determining a plurality of temporally equidistant points on the signature trace, ~~such that~~ wherein an arc length of the signature trace is a unit measurement of length and a total time to produce the signature trace is a unit measurement of time;

second extraction means for extracting second angle data and second distance data relating to different parts of the normalized signature trace, wherein the second angle data and second distance data are selected such that variance between signatures from the user is minimized and variance between signatures from other users is maximized;

registration means for storing a reference data file comprising reference angle data and reference distance data extracted from a plurality of samples of [[the]] a user's signature;

comparison means for comparing the data extracted by the second extraction means during an authentication phase to the reference angle data and the reference distance data stored in the reference data file, according to predefined verification criteria; and

verification means for generating an output indicative of a match between the user's signature and the reference angle data and the reference distance data in dependence on said comparing[[;]],

wherein the second ~~extractions~~ extraction means is implemented in a computing device.

2. (Previously presented) The system according to claim 1, wherein the second extraction means is adapted to extract data relating to a plurality of different points of the user's signature including data relating some of said points to other points in the user's signature.

3. (Currently Amended) The system according to claim 2, wherein the second extraction means is further adapted to extract data relating to a plurality of different points of the user's signature

including data relating ~~each of~~ a number of said points to an immediately preceding point in the user's signature.

4. (Currently Amended) The system according to claim 2, wherein the second extraction means is further adapted to extract data relating to a plurality of different points of the user's signature including data relating a last point to a first point in the user's signature.

5. (Currently Amended) The system according to claim 1, wherein the second extraction means includes angle extraction means for extracting angle data concerning [[the]] relative angular positions of a plurality of points of the user's signature.

6. (Currently Amended) The system according to claim 1, wherein the second extraction means includes distance extraction means for extracting distance data concerning [[the]] relative distances apart of a plurality of points of the user's signature.

7. (Currently Amended) The system according to claim 1, wherein the second extraction means includes timing extraction means for extracting timing data indicative of [[the]] relative times between execution of different parts of the user's signature, and the comparison means is adapted to compare [[the]] extracted timing data with reference timing data in the reference data file.

8. (Previously presented) The system according to claim 1, further comprising password verification means for verifying a user password.

9. (Currently Amended) The system according to claim 8, further comprising timing verification means for verifying that the user password is input in accordance with a predetermined timing.

10. (Currently Amended) The system according to claim 9, wherein the timing verification means includes means for verifying a plurality of hold times for which [[the]] relevant keys of [[the]] a keyboard input device are depressed during input of the user password, and means for verifying a plurality of latency times between a release of one key and a depression of a following key during use of the keyboard input device to enter the user password.

11. (Previously presented) The system according to claim 1, further comprising user name input means for receiving a user name.

12. (Previously presented) The system according to claim 1, wherein the comparison means incorporates at least one neural network for determining the predefined verification criteria.

13. (Currently Amended) The system according to claim 1, wherein the second extraction means is adapted to extract data relating to different features of the user's signature selected according to a fitness of such features to discriminate the user's signature for [[the]] purposes of verification and determined by a fitness function relating a relative fitness of the features to their form and number.

14. (Previously presented) The system according to claim 13, wherein the fitness function is optimized by an optimization algorithm.

15. (Currently Amended) The system according to claim 1, further comprising training means for training the system to refine the predefined verification criteria using angle and distance data relating to a plurality of samples of the user's signature inputted into the system by the user during [[the]] a registration phase and generated false samples.

16. (Previously presented) The system according to claim 1, wherein the verification means is adapted to provide an output indicative of a non-match.

17. (Currently Amended) A method ~~for authenticating a user's signature,~~ comprising:

extracting, by a computing device, first angle data and first distance data relating to different parts of [[the]] a user's signature inputted into the system by a manual input device to obtain a signature trace;

normalizing, by the computing device, the signature trace to generate a plurality of temporally equidistant points on the signature trace, ~~such that~~ wherein an arc length of the signature trace is a unit measurement of length and a total time to produce the signature trace is a unit measurement of time;

extracting, by the computing device, second angle data and second distance data relating to different parts of the normalized signature trace, wherein the second angle data and second distance

data are selected such that variance between signatures from [[the]] a user is minimized and variance between signatures from other users is maximized;

creating a reference data file comprising reference angle data and reference distance data extracted from a plurality of samples of the user's signature;

comparing, by the computing device, [[the]] data relating to different parts of the normalized signature trace during an authentication phase to the reference angle and the reference distance data stored in the reference data file, according to predefined verification criteria; and

generating an output indicative of a match between the user's signature and the reference angle data and reference distance data in dependence on said comparing.

18. (Previously Presented) The method of claim 17, wherein said extracting said first angle data and first distance data comprises extracting data relating to a plurality of different points of the user's signature including data relating some of said points to other points in the user's signature.

19. (Currently Amended) The method of claim 18, wherein said extracting said first angle data and first distance data comprises extracting data relating to a plurality of different points of the user's signature including data relating ~~each of~~ a number of said points to an immediately preceding point in the user's signature.

20. (Previously Presented) The method according to claim 18, wherein extracting said first angle data and first distance data comprises extracting data relating to a plurality of different points of the user's signature including data relating a last point to a first point in the user's signature.

21. (Currently Amended) The method of claim 17, wherein extracting said first angle data and first distance data includes extracting angle data concerning [[the]] relative angular positions of a plurality of points of the user's signature.

22. (Currently Amended) The method of claim 17, wherein extracting said first angle data and first distance data includes extracting distance data concerning [[the]] relative distances apart of a plurality of points of the user's signature.

23. (Currently Amended) The method of claim 17, wherein extracting said first angle data and first distance data includes extracting timing data indicative of [[the]] relative times between execution of

different parts of the user's signature, and said comparing further comprises comparing [[the]] extracted timing data with reference timing data in the reference data file.

24. (Currently Amended) The method of claim 17, further comprising verifying a password input.

25. (Currently Amended) The method of claim 24, further comprising verifying the password using a predefined timing.

26. (Currently Amended) The method of claim 25, wherein verifying the password input further comprises:

verifying a plurality of hold times for which [[the]] relevant keys of [[the]] a keyboard input device are depressed during input of the password; and

verifying a plurality of latency times between [[the]] a release of one key and [[the]] a depression of [[the]] a following key during use of the keyboard input device to enter the password.

27. (Previously presented) The method of claim 17, further comprising receiving a user name and using the user name to identify a reference data file.

28. (Previously presented) The method of claim 17, wherein said comparing the angle and distance data incorporates at least one neural network for determining the predetermined verification criteria.

29. (Currently Amended) The method of claim 17, wherein said extracting said first angle data and said first distance data further comprises extracting data relating to different features of the user's signature selected according to [[the]] a fitness of such features to discriminate the user's signature for [[the]] purposes of verification and determined by a fitness function relating [[the]] a relative fitness of the features to their form and number.

30. (Previously presented) The method of claim 29, wherein the fitness function is optimized by an optimization algorithm.

31. (Currently Amended) The method of claim 17, further comprising training to refine the predefined verification criteria on [[the]] a basis of angle and distance data relating to a plurality of

samples of the user's signature inputted by the user during [[the]] a registration phase and generated false samples.

32. (Previously presented) The method of claim 17, wherein said generating further comprises generating an output indicative of a non-match.

33-37. (Cancelled).

38. (Currently Amended) A non-transitory computer-readable storage medium having ~~computer-readable~~ instructions stored thereon ~~for authenticating a user's signature, the computer-readable instructions comprising:~~ the instructions comprising:

instructions for extracting first angle data and first distance data relating to different parts of a user's signature to obtain a signature trace;

instructions for normalizing the signature trace to generate a plurality of temporally equidistant points on the signature trace, ~~such that~~ wherein an arc length of the signature trace is a unit measurement of length and a total time to produce the signature trace is a unit measurement of time;

instructions for extracting second angle data and second distance data relating to different parts of [[the]] a normalized signature trace, wherein the second angle data and second distance data are selected such that variance between signatures from [[the]] a user is minimized and variance between signatures from other users is maximized;

instructions for storing a reference data file comprising reference angle data and reference distance data extracted from a plurality of samples of the user's signature;

instructions for comparing [[the]] data relating to different parts of the normalized signature trace during an authentication phase to the reference angle and the reference distance data stored in the reference data file, according to predefined verification criteria; and

instructions for generating an output indicative of a match between the user's signature and the reference angle data and reference distance data in dependence on [[said]] comparing.

39. (Currently Amended) The non-transitory computer-readable storage medium of claim 38, wherein the plurality of samples of the user's signature are normalized based, at least, upon a time to obtain a plurality of normalized samples.

40-41. (Cancelled).

42. (Currently Amended) The non-transitory computer-readable storage medium of claim 39, further comprising:

instructions for training to refine the predefined verification criteria by which a match is to be judged on [[the]] a basis of angle and distance data relating to a plurality of samples of the user's signature during [[the]] a registration phase and generated false samples.

43. (Currently Amended) A system ~~for authenticating a user's signature, the system~~ comprising:

an input apparatus~~, wherein the input apparatus is~~ configured to provide an output indicative of [[the]] a location of the input apparatus ~~with respect to time~~ when the input apparatus is manipulated;

a computing apparatus~~, wherein the computing apparatus is~~ configured to:

extract first angle data and first distance data relating to different parts of a user's signature output by the input apparatus to obtain a signature trace;

normalize the signature trace to generate a plurality of temporally equidistant points on the signature trace, ~~such that~~ wherein an arc length of the signature trace is a unit measurement of length and a total time to produce the signature trace is a unit measurement of time;

extract second angle data and second distance data relating to different parts of the normalized signature trace, wherein the second angle data and the second distance data are selected such that variance between signatures from [[the]] a user is minimized and variance between signatures from other users is maximized; and

store a reference data file comprising reference angle data and reference distance data relating to a plurality of samples of the user's signature, wherein the plurality of samples of the user's signature are normalized based upon a time to obtain a plurality of normalized samples;

a comparator apparatus configured to compare [[the]] data relating to different parts of [[the]] a normalized signature trace during an authentication phase to the reference angle and the reference distance data held in the reference data file, according to predefined verification criteria; and

an output apparatus configured to provide an output indicative of a match between the user's signature and the reference angle data and reference distance data in dependence on [[the]] a result of the comparison.

44. (Currently Amended) The system of claim 43, wherein the plurality of samples of the user's signature are normalized based, at least, upon a time to obtain a plurality of normalized samples.

45-46. (Cancelled).

47. (Currently Amended) The system of claim 44, further comprising:

a trainer configured to refine the predefined verification criteria by which a match is to be judged on [[the]] a basis of angle and distance data relating to a plurality of samples of the user's signature during [[the]] a registration phase and generated false samples.

48. (Currently Amended) A method ~~of verifying a user's signature,~~ comprising:

comparing, by a computing device, data derived from at least one vector from an input signature received from a manual input device during an authentication phase to reference angle data and reference distance data, according to predefined verification criteria, wherein the data derived from said at least one vector comprises data relating to different parts of a normalized signature trace, wherein an arc length and total time of [[the]] a signature trace are normalized to unit measurements to generate a plurality of temporally equidistant points on the signature trace, [[and]] wherein the reference angle data and reference distance data is obtained from a reference data file comprising data relating to a plurality of samples of the user's signature, wherein the plurality of samples of the user's signature are normalized based upon a time to obtain a plurality of normalized samples and selected such that variance between signatures from [[the]] a user is minimized and variance between signatures from other users is maximized; and

generating an output indicative of a match between the data derived from said at least one vector and the reference angle data and reference distance data.

49. (Currently Amended) The method of claim 48, wherein the data derived from said least one vector relates to different features of the user's signature selected according to [[the]] a fitness of such features to discriminate the user's signature for [[the]] purposes of verification and determined by a fitness function relating [[the]] relative fitness of the features to their form and number.

50. (Previously presented) The method of claim 49, wherein the fitness function is optimized by an optimization algorithm.

51. (Currently Amended) The method of claim 48, further comprising:

training to refine the predefined verification criteria by which said match is to determined.

52. (Previously presented) The method of claim 48, further comprising verifying an input of a required password, as determined by a reference password.

53. (Currently Amended) The method of claim 52, further comprising verifying the input of the required password with a required timing, as determined by a reference timing.

54. (Currently Amended) The method of claim 53, wherein verifying the input further comprises:

verifying a plurality of hold times for which relevant keys of an input device are depressed during input of the required password; and

verifying a plurality of latency times between [[the]] a release of one key and [[the]] a depression of [[the]] a following key during use of the input device to enter the required password.

55. (Currently Amended) A method ~~of verifying a signature,~~ comprising:

receiving, from a manual input device, [[the]] a signature;

extracting, by a computing device, first angle data and first distance data relating to different parts of the signature to obtain a signature trace;

normalizing, by the computing device, the signature trace to generate a plurality of temporally equidistant points on the signature trace, ~~such that~~ wherein an arc length of the signature trace is a unit measurement of length and a total time to produce the signature trace is a unit measurement of time;

extracting, by the computing device, second angle data and second distance data relating to different parts of the normalized signature trace, wherein the second angle data and second distance data are selected such that variance between signatures from [[the]] a user is minimized and variance between signatures from different users is maximized;

storing a reference data file comprising reference angle data and reference distance data extracted from a plurality of samples of [[the]] a user's signature input during a registration phase;

comparing, by the computing device, [[the]] data relating to different parts of [[the]] a normalized signature trace during an authentication phase to the reference angle data and the reference distance data stored in the reference data file, according to defined verification criteria; and

providing an output ~~to the user~~ indicative of a match between the user's signature and the reference angle data and reference distance data in dependence on [[the]] a result of said comparing.

56. (Currently Amended) The method of claim 55, further comprising linearly time warping the signature trace ~~so that~~, wherein the normalized signature trace contains a pre-determined number of temporally equidistant points.

57. (Currently Amended) The system of claim 1, wherein the first extraction means is adapted to extract ~~extracts~~ at least one vector to derive the angle data and distance data.

58. (Previously Presented) The system according to claim 1, wherein the second extraction means is adapted to extract data according to a fitness determined by applying a genetic algorithm to pairs of said temporally equidistant points.